United States Government Accountability Office

GAO

Report to the Committee on Armed Services, U.S. Senate

January 2008

DEFENSE ACQUISITIONS

Departmentwide Direction Is Needed for Implementation of the Anti-tamper Policy

GAO-08-91

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Acquistions. Departmentwide Direction Is Needed for Implementation of the Anti-tamper Policy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**25**	

January 2008

DEFENSE ACQUISITIONS

Departmentwide Direction Is Needed for Implementation of the Anti-tamper Policy

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-91, a report to the Committee on Armed Services, U.S. Senate

Why GAO Did This Study

The Department of Defense (DOD) invests billions of dollars on sophisticated weapon systems and technologies. These may be at risk of exploitation when exported, stolen, or lost during combat or routine missions. In an effort to minimize this risk, DOD developed an anti-tamper policy in 1999, calling for DOD components to implement anti-tamper techniques for critical technologies.

In March 2004, GAO reported that program managers had difficulties implementing this policy, including identifying critical technologies. This follow-up report (1) describes recent actions DOD has taken to implement its anti-tamper policy and (2) identifies challenges facing program managers.

GAO reviewed documentation on actions DOD has taken since 2004 to implement its anti-tamper policy, and interviewed officials from the Anti-Tamper Executive Agent's Office, the military services, other DOD components, and a cross-section of program offices.

What GAO Recommends

To better ensure implementation of DOD's anti-tamper policy, GAO is recommending that DOD issue departmentwide direction for its policy and provide additional tools for program managers. DOD agreed to provide additional tools to assist program managers. However, DOD believes that a directive it is currently updating addresses GAO's other concern. GAO continues to call for immediate departmentwide direction.

To view the full product, including the scope and methodology, click on GAO-08-91. For more information, contact Ann Calvaresi-Barr at (202) 512-4841 or calvaresibarra@gao.gov.

What GAO Found

Since 2004, DOD has taken several actions to raise awareness about anti-tamper protection and develop resources that provide program managers with general information on its anti-tamper policy. These actions include developing a Web site with anti-tamper information and events, establishing an online learning module on anti-tamper protection, and sponsoring research on generic anti-tamper techniques. However, DOD lacks departmentwide direction for implementation of its anti-tamper policy. Without such direction, individual DOD components are left on their own to develop initiatives. For example, the Navy is developing a database that is intended to provide a horizontal view of what DOD components have identified as critical program information. While many officials we spoke with pointed to this database as a potential tool for identifying critical technologies that may need anti-tamper protection, the database is currently incomplete. Specifically, the Missile Defense Agency is not providing information because its information is classified at a level above what the database can support. Also, the Air Force is not currently providing information because not all commands have provided consent to participate.

At the same time, program managers face challenges implementing DOD's anti-tamper policy—due largely to a lack of information or tools needed to make informed assessments at key decision points. First, program managers have limited information for defining what is critical or insight into what technologies other programs have deemed critical to ensure similar protection across programs. Determining whether technologies are critical is largely left to the discretion of the individual program manager, resulting in an uncoordinated and stove piped process. Therefore, the same technology can be identified as critical in one program office but not another. Second, program managers have not always had sufficient or consistent information from the intelligence community to identify threats and vulnerabilities to technologies that have been identified as critical. The potential impact of inconsistent threat assessments is twofold: If the threat is deemed to be low but is actually high, the technology is susceptible to tampering; conversely, if the threat is deemed to be high and is actually low, an anti-tamper solution is more robust than needed. Finally, program managers have had difficulty selecting sufficient anti-tamper solutions—in part because they lack information and tools, such as risk and cost-estimating models, to determine how much anti-tamper protection is needed. As a result, program managers may select a suboptimal solution. Given these combined challenges, there is an increased risk that some technologies that need protection may not be identified or may not have sufficient protection.

Contents

Abbreviations

AT&L	Under Secretary of Defense for Acquisition, Technology, and Logistics
DOD	Department of Defense

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 11, 2008

The Honorable Carl Levin
Chairman
The Honorable John McCain
Ranking Member
Committee on Armed Services
United States Senate

Each year, the Department of Defense (DOD) invests billions of dollars to develop and produce sophisticated weapon systems and technologies to maintain military superiority. As such, these weapons and technologies are highly sought after and at risk of exploitation when exported, stolen, or lost or damaged during combat or routine missions. Such exploitation can weaken U.S. military advantage on the battlefield and erode the U.S. industrial base's technological competitiveness in the international marketplace.

In an effort to protect U.S. weapons and technologies from exploitation, DOD established a policy in 1999 requesting each military service to implement anti-tamper techniques, which include software and hardware protective devices, when technologies are determined to be critical and vulnerable to exploitation. In March 2004, we reported on several difficulties program managers faced in implementing this policy,[1] including determining which technologies were critical—the basis for considering the need for anti-tamper protection. Difficulties with implementing DOD's anti-tamper policy, as well as vulnerabilities in related government programs, prompted GAO to designate the effective protection of technologies critical to U.S. national security as a new high-risk area in 2007.[2]

The Senate report accompanying the National Defense Authorization Act for Fiscal Year 2006 requires us to conduct a follow-up review to our March 2004 report. In response, we identified (1) recent actions DOD has

[1] GAO, *Defense Acquisitions: DOD Needs to Better Support Program Managers' Implementation of Anti-Tamper Protection*, GAO-04-302 (Washington, D.C.: Mar. 31, 2004).

[2] GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

taken to implement its anti-tamper policy and (2) challenges facing program managers.

To conduct our work, we obtained information and documentation on actions DOD has taken to implement its anti-tamper policy since 2004 and interviewed officials from the Anti-Tamper Executive Agent's Office, military services, other DOD components, and the intelligence community about these actions. We also determined the status of our 2004 report recommendations. We conducted structured interviews with officials from a cross-section of programs that the Anti-Tamper Executive Agent's Office and DOD components identified as considering and/or implementing anti-tamper protection. We discussed with these program officials their procedures for implementing anti-tamper protection and any challenges they faced. We also interviewed officials from program offices not identified by the Anti-Tamper Executive Agent and DOD components to obtain their perspective about the anti-tamper policy. We did not evaluate whether programs had implemented sufficient anti-tamper protection. We conducted this performance audit (from January 2007 to January 2008) in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. For more on scope and methodology, see appendix I.

Results in Brief

Since we reported on DOD's anti-tamper efforts in 2004, DOD has developed several anti-tamper resources to help program managers implement its anti-tamper policy—such as an online anti-tamper training course. DOD has also updated an acquisition policy document and a guidebook that provides general information on anti-tamper protection. However, DOD has not issued a formal directive or instruction incorporating its anti-tamper policy into its acquisition guidance to ensure proper implementation of the policy departmentwide. Absent clear departmentwide direction, DOD components are left to develop their own initiatives to assist in anti-tamper implementation. The extent to which DOD components will benefit from these initiatives is dependent on acceptance and adoption by all, which has yet to occur.

A lack of information or tools at three key decision points—identifying critical technologies, threats and vulnerabilities, and solutions—has significantly challenged program managers in effectively implementing

DOD's anti-tamper policy. First, program managers have limited information for defining what is critical or insight into what technologies other programs have identified as critical to ensure similar protection across programs. Second, program managers have not always had sufficient or consistent information from the intelligence community to identify threats and vulnerabilities to critical technologies. Third, program managers have had difficulty selecting solutions, in part because they lack the information and tools, such as risk and cost-estimating models, to determine how much anti-tamper protection is needed to protect critical technologies. Given these challenges, some technologies that need protection may not be identified or may not be sufficiently protected.

We are recommending that DOD take actions to establish departmentwide direction that prescribes how to carry out its anti-tamper policy and identify and provide additional tools to assist program managers during key decision points.

In written comments on a draft of this report, DOD concurred with our recommendation to provide additional tools to assist program managers in their anti-tamper decision process but nonconcurred with our recommendation that the Under Secretary of Defense for Acquisition, Technology, and Logistics provide specific direction on applying its anti-tamper policy. DOD stated that the Under Secretary of Defense (Intelligence) is currently updating the security and counterintelligence support directive to acquisition programs. Following the update, DOD plans to update a manual with a new section explicitly for anti-tamper protection. We continue to believe that direction on applying anti-tamper policy has long been needed and should not be delayed and that the Under Secretary of Defense for Acquisition, Technology, and Logistics, who is responsible for anti-tamper policy, should be involved in developing and providing direction.

Background

To protect its critical assets, DOD has established several protection measures for weapon systems. These measures include information assurance to protect information and information systems, software protection to prevent the unauthorized distribution and exploitation of critical software, and anti-tamper techniques to help delay exploitation of

technologies through means such as reverse engineering[3] when U.S. weapons are exported or lost on the battlefield. Examples of anti-tamper techniques include software encryption, which scrambles software instructions to make them unintelligible without first being reprocessed through a deciphering technique, and hardware protective coatings designed to make it difficult to extract or dissect components without damaging them.[4]

In 1999, the Under Secretary of Defense for Acquisition, Technology, and Logistics (AT&L) issued a policy memorandum for implementing anti-tamper protection in acquisition programs. In the following year, AT&L issued a policy memorandum stating that technologies should be routinely assessed during the acquisition process to determine if they are critical and if anti-tamper techniques are needed to protect these technologies. In 2001, an AT&L policy memorandum designated the Air Force as the Anti-Tamper Executive Agent. The executive agent's office, which currently has four staff, is responsible for implementing DOD's anti-tamper policy and managing anti-tamper technology development through the Air Force Research Laboratory. The executive agent also holds periodic information sessions to educate the acquisition community about anti-tamper policy, initiatives, and technology developments. To coordinate activities, military services and defense agencies, such as the Missile Defense Agency, have an anti-tamper point of contact. Program managers are responsible for ensuring anti-tamper protection is incorporated on any weapon system with critical technologies that need protection.[5] Since it is not feasible to protect every technology, program managers are to conduct an assessment to determine if anti-tamper protection is needed.

[3] Reverse engineering is the process of taking apart an item such as hardware or software to see how it works. For example, a software program may be reverse engineered to determine how the program performs certain operations.

[4] Information regarding the specific anti-tamper solutions used on an individual system is typically classified because disclosure could aid exploitation. In some cases, anti-tamper information is restricted at the special access level.

[5] According to guidelines accompanying the 2000 AT&L policy memorandum, anti-tamper should be considered for all new start programs; programs that did not reach systems development prior to May 1, 2000; and all preplanned product improvement, modifications, or other technology insertion efforts. In addition, anti-tamper should be considered for all foreign military sales or direct commercial sales and for all upgrades to all programs, regardless of when systems development occurred.

When assessing if anti-tamper protection is needed, program managers make several key decisions regarding the identification of critical technologies, assessment of threats and vulnerabilities, and determination of anti-tamper techniques or solutions. The process begins with determining whether or not their system's critical program information[6] includes any critical technologies. If it is determined that the system has no critical technologies, program managers are to document the decision and request concurrence from either the office within their component that is designated with anti-tamper responsibilities or the Anti-Tamper Executive Agent. For systems that are determined to have critical technologies, the next key steps are to identify potential threats and vulnerabilities and select anti-tamper techniques to protect those technologies. Techniques are ultimately verified and validated by a team[7] composed of representatives from the DOD components. The program manager documents decisions in an annex of the program protection plan.[8]

In 2004, we reported that program managers had difficulty in carrying out DOD's anti-tamper policy on individual weapons, such as identifying critical technologies and experiencing cost increases or schedule delays when applying anti-tamper techniques—particularly when the techniques are not fully developed or when the systems are already in design or production. We made several recommendations, including increasing oversight over the identification of critical technologies across programs, improving tools and resources for program managers in identifying critical technologies, ensuring early identification of anti-tamper costs and solutions, monitoring the development of generic anti-tamper solutions and evaluating their effectiveness, and developing a business case to determine whether the current organizational structure and resources are adequate. DOD concurred or partially concurred with these recommendations. DOD has taken some steps to implement our

[6] Critical program information is information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat effective life of the system, or significantly alter program direction.

[7] A validation and verification team validates that a program office's anti-tamper implementation will fulfill its intended function and verifies that anti-tamper measures stipulated in the anti-tamper plan operate according to specifications.

[8] A program protection plan is a program manager's single source document used to coordinate and integrate all protection efforts designed to deny access to critical program information to anyone not authorized or not having a need to know and prevent inadvertent disclosure of leading edge technology to foreign interests.

recommendations including identifying available anti-tamper technical resources and developing a searchable spreadsheet of critical technologies, incorporating information in the *Defense Acquisition Guidebook* on the need for early identification of anti-tamper solutions in a weapon system, and sponsoring a study on anti-tamper techniques and their general effectiveness. While DOD has taken these steps to address parts of the recommendations, all remain open.

DOD Lacks Departmentwide Direction for Implementing its Anti-tamper Policy

DOD has recently taken several actions aimed at raising awareness about its anti-tamper policy and assisting program managers in implementing anti-tamper protection on a weapon system. Despite these actions, DOD still lacks departmentwide direction to implement its anti-tamper policy. Without such direction, DOD components are left to develop their own initiatives to assist program managers in implementing anti-tamper protection. While individual efforts are important, such as a database to track critical program information DOD-wide, their effectiveness may be limited because they have yet to be accepted and adopted across all DOD components.

DOD Has Developed Some Resources for Program Managers to Use in Implementing Anti-tamper Protection

Since our 2004 report, DOD, through the Anti-Tamper Executive Agent, has developed some resources aimed at assisting program managers as they go through the anti-tamper decision process. DOD's resources range from providing general information about the anti-tamper policy to research on anti-tamper solutions. Specifically, DOD has

- developed a guidebook that includes a checklist to assist program managers in identifying security, management, and technical responsibilities when incorporating anti-tamper protection on a weapons system;
- developed a searchable spreadsheet to assist program managers in identifying critical technologies;
- developed a Web site for program managers to provide general anti-tamper information, policy resources, conference briefings, implementation resources, and current events;
- coordinated with Defense Acquisition University to design and launch an online learning module on anti-tamper protection;
- funded Sandia National Laboratories to study anti-tamper techniques and their general effectiveness; and
- sponsored research to develop generic anti-tamper techniques through Small Business Innovation Research, a research program that funds early-stage research and development projects at small technology companies.

DOD has also updated two acquisition documents with general anti-tamper information. The first document—DOD Instruction 5000.2, Operation of a Defense Acquisition System—currently states that one of the purposes of the System Development and Demonstration phase of a weapon system is to ensure affordability and protection of critical program information by implementing appropriate solutions such as anti-tamper protection. The second document—the *Defense Acquisition Guidebook*—has been updated to include some basic information on the importance of implementing anti-tamper protection early in the development of a weapon system and describes program managers' overall responsibilities for implementing the anti-tamper policy.

DOD Has Not Provided Direction to Implement Its Anti-tamper Policy

While DOD has issued broad policy memorandums that reflect the department's desire for routinely assessing weapon systems to determine if anti-tamper protection is needed, the department has not fully incorporated the anti-tamper policy into its formal acquisition guidance. Specifically, DOD Instruction 5000.2 mentions anti-tamper protection, but the department has not provided direction for implementation of anti-tamper in a formal directive or instruction. Currently, the department is coordinating comments on a draft instruction (DOD Instruction 5200.39) on protection of critical program information that includes anti-tamper implementation.[9] However, in commenting on the draft instruction, several DOD components have raised concerns about when and how to define critical program information that warrants protection, which have contributed to long delays in finalizing the instruction. In addition, the department has not provided specific guidance for program managers on how to implement anti-tamper protection in a DOD manual because DOD officials said this process cannot begin until the instruction is finalized. The date for finalizing the instruction has not yet been determined.

Officials from the executive agent's office stated that departmentwide direction would give credence to the anti-tamper policy in practice. Anti-tamper points of contact told us that the policy memorandums are not sufficient to ensure that program managers are implementing anti-tamper protection on weapon systems when necessary. One service anti-tamper point of contact stated that program managers might disregard the policy memorandums because they are high-level and broad. Another service anti-tamper point of contact said that implementation is ultimately left up

[9] According to DOD, the department began this process in 1999.

to the individual program manager. While a program manager's decision should be approved by the milestone decision authority[10] and documented in the program protection plan, some service and program officials said that programs are not always asked about anti-tamper protection during the review.

Absent Departmentwide Direction, Components Have Been Left to Develop Their Own Anti-tamper Initiatives

Lacking departmentwide direction for the anti-tamper policy, DOD components have been left to develop their own initiatives to assist program managers in anti-tamper implementation. However, the usefulness of these initiatives depends on the extent to which other components participate in these efforts.

For example, the Missile Defense Agency developed a risk assessment model to help program managers identify how much anti-tamper is needed to protect critical technologies. Specifically, the model helps program managers assess the criticality of the technology relative to the risk of exploitation. However, when the Missile Defense Agency sought comments on the initiative, the executive agent and services indicated that it was too lengthy and complex to use. The executive agent, in coordination with anti-tamper points of contact from the Missile Defense Agency and services, has taken over this effort, and it is still in development.

The Navy is also implementing an initiative: a database intended to capture the information that programs across DOD components have identified as critical. Many officials we spoke with pointed to this database as a potential tool to improve identification of critical program information across DOD components. To date, the Navy and the Army are submitting information for the database, but the Missile Defense Agency and Air Force are not. The Missile Defense Agency anti-tamper point of contact stated that its information is classified at a level above what the database can support and its program managers will not submit information for the database unless DOD requires submissions by all DOD components. However, the Missile Defense Agency does have access to the database and uses it as a cross-check to determine if it is identifying similar critical program information. The Air Force has been briefed on the initiative but

[10] The milestone decision authority is a designated DOD individual with the authority to approve entry of an acquisition program into the next phase of the acquisition process and is accountable for cost, schedule, and performance reporting to a higher authority, including congressional reporting.

does not yet have consent from all of the commands to participate. Without full participation across all DOD components, the usefulness of this database as a tool to identify critical technologies that may need anti-tamper protection will be limited.

Program Managers Face Several Challenges in Identifying Critical Technologies, Threats, and Sufficient Anti-tamper Solutions

To determine whether anti-tamper protection is needed, program managers must identify which technologies are deemed critical, determine the potential threats and vulnerabilities to these technologies, and identify sufficient anti-tamper solutions to protect the technologies. Such decisions involve a certain level of subjectivity. However, program managers lack the information or tools needed to make informed assessments at these key decision points. As a result, some technologies that need protection may not be identified or may not have sufficient protection.

Limited Information and Coordination on What Is Critical Increase the Risk That Some Technologies May Not Be Identified

Determining technologies that are critical is largely left to the discretion of the program managers. While DOD has some resources available to program managers to help identify critical technologies, they may be of limited use. For example, the executive agent's searchable spreadsheet of critical technologies may not be comprehensive because it relies on DOD's Militarily Critical Technologies List, which we reported in 2006 was largely out of date.[11] Also, some program offices have used a series of questions established in a 1994 DOD manual on acquisition systems protection to help guide their discussions on what is critical. However, these questions are broad and subject to interpretation, and can result in different conclusions, depending on who is involved in the decision-making process.

In addition, identifying what is critical varies by DOD component and sometimes by program office. For example, one Air Force program office

[11] The spreadsheet is based primarily on the Militarily Critical Technologies List—a compendium of goods and technologies that would permit significant advances in military capabilities in the near term—and the Developing Science and Technologies List—a compendium of scientific and technological capabilities being developed worldwide that could affect U.S. military capabilities in the long term. In 2006, we reported that both lists are largely out of date and are of questionable value. GAO, *Defense Technologies: DOD's Critical Technologies Lists Rarely Inform Export Control and Other Policy Decisions*, GAO-06-793 (Washington, D.C.: July 28, 2006).

tried various approaches, including teams of subject matter experts, over 2 years to identify its list of critical program information. In contrast, the Army took the initiative to establish a research center to assist program managers in identifying critical program information, but Army officials stated that the approach used by the center has led to an underestimating of critical program information and critical technologies in programs.

At the same time, there has been limited coordination across programs on technologies that have been identified as critical—creating a stove piped process—which could result in one technology being protected under one program and not protected under another. While informal coordination can occur, programs did not have a formal mechanism for coordinating with other programs, including those within their service. For example, officials from one program office stated they had little interaction from programs within their service or other services to ensure protection of similar technologies. A program under one joint program executive office had not coordinated with other programs to identify similar technologies as critical. In addition, according to an Army official, contractors who have worked on programs across services have questioned why one service is applying anti-tamper solutions to a technology that another service has not identified as critical. Finally, one program office we spoke with identified critical program information on its system but indicated that a similar system in another service had not identified any critical program information and, therefore, had no plans to implement anti-tamper protection.

Despite the risk that some technologies that need protection may not be identified or may not be protected across programs, no formal mechanism exists within DOD to provide a horizontal view of what is critical.[12] However, any effort to do so could be undermined by the programs' and services' different definitions and interpretations of "critical program information" and "critical technologies." The Anti-Tamper Executive Agent defines critical program information as capturing all critical technologies. In contrast, the Army's interpretation is that critical program information only includes critical technologies that are state-of-the-art. For the Navy, critical program information includes software, while hardware is part of what the Navy defines as critical technologies. One program that is part of

[12] In our March 2004 report (GAO-04-302) we recommended that DOD improve its oversight of the identification of critical technologies by all programs subject to the anti-tamper policy.

a joint program office identified critical program information as including company proprietary information. As a result, tracking critical program information may not provide a horizontal view of all technologies services and programs have identified as needing anti-tamper protection.

Contradictory and Insufficient Intelligence Information Has Hindered Some Programs in Identifying Potential Threats

Once a program office identifies critical technologies, the next step in the anti-tamper decision process is to identify threats to those technologies. DOD's *Program Manager's Guidebook and Checklist for Anti-tamper* states that multiple threat assessments should be requested from either the service intelligence organization or counterintelligence organization. One program office we visited stated that it has requested and received multiple threat assessments from the intelligence community, which have sometimes contradicted one another, leaving the program office to decipher the information and determine the threat. According to an anti-tamper point of contact, other programs have received contradictory information—typically relating to foreign countries' capabilities to reverse engineer. The potential impact of contradictory intelligence reports is twofold: If the threat is deemed to be low but is actually high, the technology is susceptible to reverse engineering; conversely, if the threat is deemed to be high and is actually low, the anti-tamper solution is more robust than needed.

To assist with the process of identifying threats, program offices may request threat assessments from a group within the Defense Intelligence Agency. However, this group was not able to complete assessments for approximately 6 months during 2006. While the group has resumed completing assessments, an agency official stated that it is not able to produce as many assessments as before due to limited resources. The Defense Intelligence Agency does not turn down program offices that may request assessments, but does have to put them in a queue and provide them with previous assessments, if they exist, until it can complete a full assessment for the program office. One program office indicated that it took 6 to 9 months for the agency to complete its assessment.

Program Managers Need Tools to Assist in Designing Effective Anti-tamper Solutions and Estimating Related Costs

Program managers also lack the tools needed to identify the optimal anti-tamper solutions for those critical technologies that are vulnerable to threats. Most notably, program managers lack a risk model to assess the relative strengths of different anti-tamper solutions and a tool to help estimate their costs.

According to National Security Agency officials, who are available to provide support to program managers considering or implementing anti-tamper protection, program managers and contractors sometimes have difficulty determining appropriate solutions. Four of five programs we spoke with that had experience in this area of the anti-tamper decision process had difficulty identifying how much anti-tamper protection was enough to protect a critical technology. For example, one program official told us that an anti-tamper solution developed for one of the program's critical technologies may not be sufficient to prevent reverse engineering. Another program office stated that it is difficult to choose between competing contractors without knowing how to determine the appropriate level of anti-tamper protection needed. An anti-tamper point of contact said that program managers need a tool to help them assess the criticality of a technology versus the types of threats to that technology.

Implementing a suboptimal anti-tamper solution can have cost and performance implications for the program. Specifically, if the solution provides less anti-tamper protection than is needed, the program may have to retrofit additional anti-tamper protection to allow for a more robust solution. Not only can such retrofitting add to a program's costs, it can compromise performance.

Given limited resources and tools for determining anti-tamper solutions, some program office officials told us that to satisfy anti-tamper solutions they relied on other protection measures. For example, officials in one program office stated that anti-tamper protection and information assurance[13] were interchangeable and indicated that following the National Security Agency's information assurance requirements—which number in the hundreds—should be sufficient as an anti-tamper solution for this system. This same program was not aware of anti-tamper resources and did not coordinate with an anti-tamper validation and verification team on its solutions. Also, an official from another program office indicated that anti-tamper protection and information assurance are similarly defined. While DOD and service officials agreed that some information assurance and anti-tamper measures may overlap, fulfilling information assurance requirements does not guarantee a sufficient anti-tamper solution.

[13] Information assurance refers to measures that defend and protect information and information systems by ensuring their confidentiality, integrity, authenticity, availability, and utility.

Conclusions

In establishing various policies to protect its critical assets, DOD saw anti-tamper as a key way to preserve U.S. investment in critical technologies while operating in an environment of coalition warfare and a globalized industry. Program managers are ultimately responsible for implementing DOD's anti-tamper policy. However, a lack of direction, information, and tools from DOD to implement its policy has created significant challenges for program managers. Further, this policy can compete with the demands of meeting program cost and schedule objectives, particularly when the optimal anti-tamper solution is identified late in the schedule. Until DOD establishes a formal directive or instruction for implementing its policy departmentwide and equips program managers with adequate implementation tools, program managers will continue to face difficulties in identifying critical technologies and implementing anti-tamper protection.

Recommendations for Executive Action

As DOD examines its policies for protecting critical assets, we are recommending that the Secretary of Defense direct the Under Secretary of Acquisition, Technology, and Logistics, in coordination with the Anti-Tamper Executive Agent and the Under Secretary of Defense for Intelligence, to issue or be involved in developing and providing departmentwide direction for application of its anti-tamper policy that prescribes how to carry out the policy and establishes definitions for critical program information and critical technologies.

To help ensure the effectiveness of anti-tamper implementation, we also recommend that the Secretary of Defense direct the Anti-Tamper Executive Agent to identify and provide additional tools to assist program managers in the anti-tamper decision process.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD concurred with our recommendation that the Secretary of Defense direct the Anti-Tamper Executive Agent to identify additional tools to assist program managers in the anti-tamper decision process. DOD stated that the Anti-Tamper Executive Agent is drafting Anti-Tamper Standard Guidelines to facilitate proper implementation of anti-tamper protection across the department.

DOD did not concur with our recommendation that the Secretary of Defense direct the Under Secretary of Defense (AT&L) in coordination with the Anti-Tamper Executive Agent and the Under Secretary of Defense (Intelligence) to issue departmentwide direction for application of its anti-tamper policy that prescribes how to carry out the policy and establishes

definitions for critical program information and critical technologies. DOD stated that the Under Secretary of Defense (Intelligence) has primary responsibility for DOD Directive 5200.39, a security and counterintelligence support directive to acquisition programs, and its successor, DOD Instruction 5200.39 regarding protection of critical program information. The Under Secretary of Defense (Intelligence) is currently coordinating an update to this directive. Once it is issued, the department plans to update DOD 5200.1-M, which provides the execution standards and guidelines to meet the DOD Instruction 5200.39 policy.

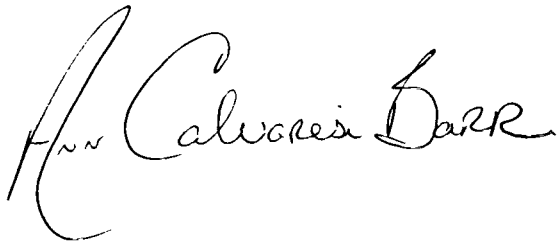
While DOD has issued broad policy memorandums beginning in 1999 that reflect the department's desire for routinely assessing weapon systems to determine if anti-tamper protection is needed, the department has not fully incorporated anti-tamper policy into its formal acquisition guidance. As we have reported, service officials indicated collectively that these policy memorandums are high-level, broad, and leave implementation ultimately up to the individual program manager. DOD did not indicate when the update of DOD Directive 5200.39 might be complete and guidance on anti-tamper implementation issued. We continue to believe that such direction is currently needed and that the Under Secretary of Defense for Acquisition, Technology, and Logistics, who issued the policy memorandums and is responsible for anti-tamper policy, should be involved in developing and providing the appropriate direction whether it be the update to DOD Directive 5200.39 or another vehicle. That direction should include how to implement the anti-tamper policy and how critical program information and critical technologies are defined. We continue to believe that the direction, which has been lacking since the policy was initiated in 1999, should not be further delayed. If DOD continues to experience delays in updating DOD Directive 5200.39, it should consider interim measures to meet the immediate need for anti-tamper direction.

DOD's letter is reprinted in appendix II.

We are sending copies of this report to interested congressional committees, as well as the Secretary of Defense; the Director, Office of Management and Budget; and the Assistant to the President for National Security Affairs. In addition, this report will be made available at no charge on the GAO Web site at http://www.gao.gov.

Please contact me at (202) 512-4841 or calvaresibarra@gao.gov if you or your staff have any questions concerning this report. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Others making key contributions to this report are listed in appendix III.

Sincerely yours,



Ann Calvaresi-Barr
Director
Acquisition and Sourcing Management

Appendix I: Scope and Methodology

To identify actions the Department of Defense (DOD) has taken to implement its anti-tamper policy since 2004, we reviewed DOD policies and guidance governing anti-tamper protection on weapon systems and obtained documents on various initiatives. We interviewed officials from the Anti-Tamper Executive Agent, military services, and other DOD components such as the Missile Defense Agency; Acquisition, Technology and Logistics; Defense Intelligence Agency; National Security Agency; and the Air Force Research Laboratory about initiatives or actions taken regarding anti-tamper. Through these interviews and documents, we also determined the status of our 2004 anti-tamper report recommendations. We interviewed DOD officials from Networks and Information Integration, Science and Technology, and Counterintelligence to discuss anti-tamper protection and how it relates to other program protection measures.

To determine how program managers implemented DOD's anti-tamper policy, we interviewed officials from 14 program offices. We are not identifying the names of the programs due to classification concerns. We conducted structured interviews with 7 of the 14 program offices to discuss and obtain documents about their experiences with implementing the anti-tamper decision process and identify any challenges they faced. We selected 6 of these programs from a list of weapon systems identified in Anti-Tamper Executive Agent, services, and component documents as considering and/or implementing anti-tamper protection and a seventh program considering anti-tamper that we identified during the course of our fieldwork. Systems we selected represented a cross section of acquisition programs and various types of systems in different phases of development. For the remaining programs, we interviewed 7 not identified by the Anti-Tamper Executive Agent or the services as considering and/or implementing anti-tamper to obtain their viewpoints on DOD's anti-tamper policy and implementation. We selected these programs by identifying lists of DOD acquisition programs and comparing them to the Anti-Tamper Executive Agent's, services', and components' lists of program considering and/or implementing anti-tamper. We did not evaluate whether programs had implemented sufficient anti-tamper protection.

Appendix II: Comments from the Department of Defense

DEPUTY UNDER SECRETARY OF DEFENSE
3015 DEFENSE PENTAGON
WASHINGTON, DC 20301-3015

ACQUISITION AND TECHNOLOGY

DEC 20 2007

Ms. Calvaresi-Barr
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Calvaresi-Barr:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-08-91SU, "DEFENSE ACQUISITIONS: Department-wide Direction Is Needed for Implementation of the Anti-tamper Policy," dated October 17, 2007 (GAO Code 120611).

Sincerely,

Mark D. Schaeffer
Director
Systems and Software Engineering

Enclosure:
As stated

GAO DRAFT REPORT DATED OCTOBER 17, 2007
GAO-08-91SU (GAO CODE 120611)

"DEFENSE ACQUISITIONS: DEPARTMENTWIDE DIRECTION IS NEEDED FOR IMPLEMENTATION OF THE ANTI-TAMPER POLICY"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense direct the Under Secretary of Defense (Acquisition, Technology, and Logistics), in coordination with the Anti-Tamper Executive Agent and the Under Secretary of Defense (Intelligence), to issue department-wide direction for application of its anti-tamper policy that prescribes how to carry out the policy and establishes definitions for critical program information and critical technologies. (p. 13/GAO Draft Report)

DOD RESPONSE: Non-concur. The Under Secretary of Defense (Intelligence) (USD(I)) is the office of primary responsibility for DoDD 5200.39, "Security Intelligence, and Counterintelligence Support to Acquisition Program Protection," and its successor, DoDI 5200.39, "Critical Program Information (CPI) Protection within the Department of Defense." USD(I) is currently coordinating an update to the directive.

The Anti-Tamper Executive Agent (ATEA) has proposed the incorporation of anti-tamper policy in this revision. The considered policy for anti-tamper mandates:

> "For critical technology type CPI, employ appropriate anti-tamper during the RDA process unless waived in writing by MDA or equivalent."

Following the issuance of the updated DoDI 5200.39, the Department will revised the DoD 5200.1-M, "Acquisition Systems Protection," the implementing manual for the directive which provides the execution standards and guidelines to meet the DoDI 5200.39 policy. The ATEA's plan is to include a new section in the manual that is explicitly for anti-tamper. This will describe how to implement anti-tamper to protect technology CPI for U.S.-only cases, foreign military sales/direct commercial sales, and science and technology programs.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense direct the Anti-Tamper Executive Agent to identify and provide additional tools to assist program managers in the anti-tamper decision process. (p. 13/GAO Draft Report)

DOD RESPONSE: Concur. The ATEA is drafting a classified document called the Anti-Tamper Standard Guidelines. This document will assist program personnel in understanding how their system might be exposed to adversaries and the consequence of technology CPI compromise. These guidelines will facilitate proper implementation of AT protection of identified technology CPI. The document will define AT protection expectations and will help program personnel understand the rough magnitude of AT protection required to field the system and also to estimate the cost of AT prior to Milestone B. This information can also provide the basis for identification of AT protection requirements to potential contractors during a Request for Proposal. The document, by providing standard anti-tamper guidelines for all programs to follow, will help implement horizontal protection of technology CPI across the department.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Ms. Ann Calvaresi-Barr (202) 512-4841 or calvaresibarra@gao.gov

Acknowledgments

In addition to the contact named above, Anne-Marie Lasowski (Assistant Director), Gregory Harmon, Molly Whipple, Karen Sloan, John C. Martin, and Alyssa Weir made major contributions to this report.

Related GAO Products

High-Risk Series: An Update. GAO-07-310. Washington, D.C.: January 2007.

Export Controls: Challenges Exist in Enforcement of an Inherently Complex System. GAO-07-265. Washington, D.C.: December 20, 2006.

Defense Technologies: DOD's Critical Technologies Lists Rarely Inform Export Control and Other Policy Decisions. GAO-06-793. Washington, D.C.: July 28, 2006.

President's Justification of the High Performance Computer Control Threshold Does Not Fully Address National Defense Authorization Act of 1998 Requirements. GAO-06-754R. Washington, D.C.: June 30, 2006.

Export Controls: Improvements to Commerce's Dual-Use System Needed to Ensure Protection of U.S. Interests in the Post-9/11 Environment. GAO-06-638. Washington, D.C.: June 26, 2006.

Defense Trade: Enhancements to the Implementation of Exon-Florio Could Strengthen the Law's Effectiveness. GAO-05-686. Washington, D.C.: September 28, 2005.

Industrial Security: DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient. GAO-05-681. Washington, D.C.: July 15, 2005.

Defense Trade: Arms Export Control Vulnerabilities and Inefficiencies in the Post-9/11 Security Environment. GAO-05-468R. Washington, D.C.: April 7, 2005.

Defense Trade: Arms Export Control System in the Post-9/11 Environment. GAO-05-234. Washington, D.C.: February 16, 2005.

Defense Acquisitions: DOD Needs to Better Support Program Managers' Implementation of Anti-Tamper Protection. GAO-04-302. Washington, D.C.: March 31, 2004.

Defense Trade: Better Information Needed to Support Decisions Affecting Proposed Weapons Transfers. GAO-03-694. Washington, D.C.: July 11, 2003.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, jarmong@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548